Defence Research and Development Canada
Recherche et développement pour la défense Canada

DRDC | RDDC
technologyscience technologie

2014-08-21

DRDC-RDDC-2014-L280

Distribution List

Scientific Letter

On the suitability of radios that interface with tactical apps on Android OS

Background

This Scientific Letter (SL) is written as a summary for a DRDC Contract Report (CR) entitled Emerging Radio and MANET Technology Study, DRDC-RDDC-2014-C14-0717-1208, and its influence on de-risking current research activities.

There is an emerging trend in military tactical networks to equip users at the tactical edge with sophisticated information technology devices capable of providing situational awareness updates using high-bandwidth short-hop networking. In Canada, for instance, the Integrated Soldier Systems Program (ISSP) capital project is intending to deliver hand-held situational awareness display devices to dismounted soldiers to improve survivability and navigation. Internationally, researchers are exploring the military utility of applications (apps) on mobile devices using commercial-off-the-shelf (COTS) operating systems (OS) such as iOS[1] and Android OS [1-5]. This trend is fueled by the familiarity of a new generation of end users with smart phone and tablet technology, as well as by the increasingly fast-to-market speed of the technologies. It is not unreasonable to expect that adversaries—especially asymmetric threats—are actively following these developments with an interest in exploiting inexpensive COTS products to further their own ends as well.

With an eye on these trends towards a network-enabled capability, the Tactical Edge Cyber Command and Control (TEC3) project initiated by Defence Research and Development Canada (DRDC) is developing a software tool suite for tactical edge networks. The tool suite will provide mobile device apps for network and security situational awareness (SA), network management and command and control (C2), and full-spectrum cyber operations. In conducting preliminary research for TEC3, we observed that the focus of many mobile device projects is on application development with little regard to the radios providing the network (and their limitations), often making the tacit assumption that the apps are radio agnostic. However, in the TEC3 concept of operations [6], we identified a number of scenarios and use cases in which it would be beneficial for a mobile display device to be able to engage in low-level interactions with a tethered radio, as opposed to simply using the radio as a networking tool. To exchange simple situational awareness information it is sufficient to view the radio strictly as a communications pipe; however, to efficiently manage the network, optimize it for mission constraints, and conduct cyber operations, a two-way exchange of protocol information between the radio and the display device is desirable, as depicted in Figure 1.

[1] The "i" is commonly understood as a trademark for Apple Inc. products as in iPhone, iPad, and iPod.

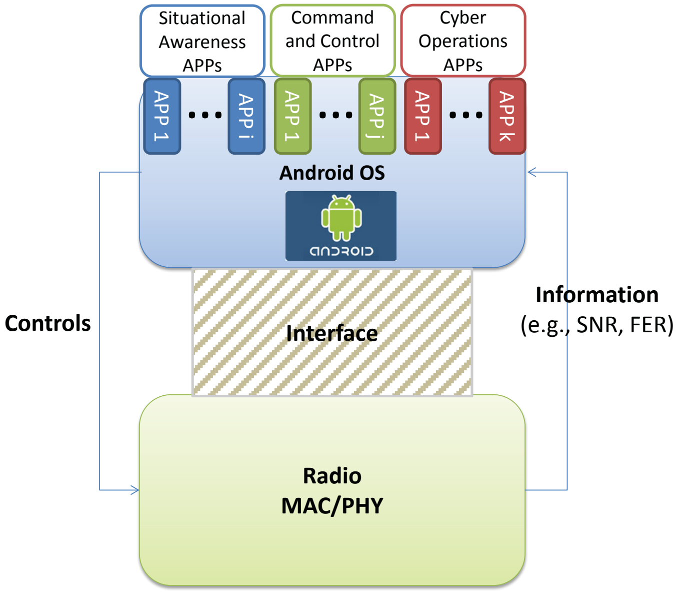

Figure 1: *A block diagram of the interdependencies between a radio and an Android OS display device on which APPs are built.*

As a first step in specifying TEC3 hardware requirements, DRDC's Cyber Operations and Signals Warfare (COSW) Section funded a contract [7] to assess the viability of leveraging COTS computing tablets (e.g., Android tablets or smart phones) to control and interface with longer-range radio platforms (either military or commercial) as part of a mobile ad hoc network (MANET).

As a starting point for the contractor's study, DRDC proposed the high-level architecture shown in Figure 1. It includes a radio component for communications and establishing the network; a display/GUI component for visual situational awareness and management of the network; and an interface between the two allowing for protocol information exchange. It was recognized from the outset that these three elements could be integrated into the same device[2], or the components could be tethered together such that a display interface is used to control an external radio (e.g., a military-off-the-shelf (MOTS) tactical radio plugged into a COTS tablet-like display through Universal Serial Bus - USB).

The contractor surveyed existing tablet and radio technologies, investigating the performance and specifications of multiple platforms "out of the box". They reported on the ease with which the platforms could be modified or augmented with custom software and applications using existing hardware and software interfaces, application programming interfaces (API), software development kits (SDK), and driver development kits (DDK). The ability to modify and customize radio and/or tablet functionality was of particular interest to DRDC, with the understanding that some of the advanced C2 and cyber operations envisioned for TEC3 will require a degree of modifications to out-of-the-box functionality.

The contractor's survey covered military, commercial, and open-source radios, as shown in Figure 2. They investigated six possible architectures for connecting and managing an Android tablet/radio/interface system. The technical ease with which these radios (or their sockets and

[2] For instance, a COTS tablet consists of a tablet display with an integrated 802.11 radio. However, while typical COTS tablets are easily programmable and support myriad applications, the integrated radios are generally short-range (e.g., 802.11 Wi-Fi radios with ranges less than 200 m), whereas military radios may require ranges well over 1000 m.

interfaces to a tablet) could be modified to add additional functionality provided a criterion to eliminate several possible architectural configurations for a “radio-plus-tablet” device. We now better understand how a COTS/MOTS radio-plus-tablet device could be established and used as a platform on which to build a tactical network with modular (app-like) command and control (C2), situational awareness (SA), and cyber operations applications.

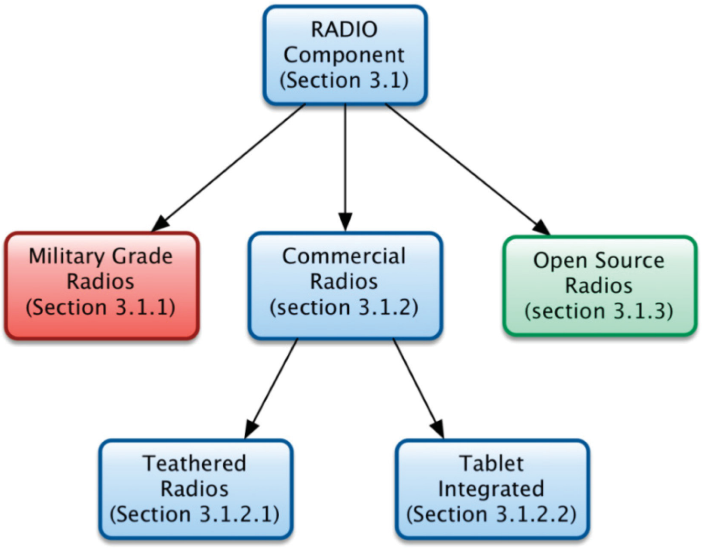
RADIO Component (Section 3.1)
Military Grade Radios (Section 3.1.1)
Commercial Radios (section 3.1.2)
Open Source Radios (section 3.1.3)
Teathered Radios (Section 3.1.2.1)
Tablet Integrated (Section 3.1.2.2)

Figure 2: *A tree diagram from [7] showing the coverage of the radio-plus-tablet study contract.*

Statement of results

Based on the results of our contracted survey, there are three viable configurations for a radio-plus-tablet device that could be used as a platform for a MANET with tactical C2 and SA apps. The three configurations vary in their technical readiness levels (TRL) in providing an in-the-field functionality to an end user at the tactical edge.

1. The solution with the lowest TRL, but one that is beneficial for DRDC COSW experimental research, is an open source software defined radio (SDR) that interfaces with a tablet (or a PC) via a Universal Serial Bus (USB) interface and is programmed/configured using device drivers, firmware, and open source software such as GNURadio. Examples of this type of radio include the HackRF, BladeRF, and the Universal Software Radio Peripheral (USRP), respectively listed in a decreasing order of commercialization, ease of use, and product user friendliness. These devices all have inputs for external antennae to extend their range and capabilities.

2. A mid-TRL configuration is offered by a fully commercialised product, in the form of a USB ”radio on a stick”, which also comes with open source device drivers and firmware as well as input for external antenna. One such product is the TP-LINK TL-WN722N wireless network adapter. This configuration is useful for COSW trials and demonstrations of innovative research solutions that can be loaded as software on either the tablet or the radio. Although the product uses an 802.11 radio making it less desirable for a military deployment, its open architecture and programmability make it a good candidate for cyber research demonstrations, where the exact physical layer employed is not the primary concern.

3. The highest TRL configuration (which is also considerably more expensive), is to opt for a proprietary solution such as those offered by typical COTS military vendors. One example

solution of this type is the Persistent Systems Man Portable Unit Gen4 combined with the Android Kit to supply connectivity to a tablet. This military contractor is capable of frequent, customizable firmware updates, incorporating emerging requirements from clients. They can also alter radio components (e.g., chipsets) and interfaces (e.g., IP wireless networking or USB tethering). While this option will yield the most “fieldable” result, it may limit flexibility of a research demonstration.

Discussion of results

COSW is interested in an experimental interconnectivity of a combination of the first two configurations because of the flexibility these configurations allow for testing and developing new cyber capabilities. The third option above is the best choice for formal accreditation and a capital acquisition project, however may offer less R&D flexibility (in addition to a much larger acquisition cost).

We believe that studying the interconnectivity of the following radio-plus-tablet instances in an 802.11 test bed would be useful de-risking activities to support the tasks under the Tactical Network Operations (TNO) project (an omnibus project comprising TEC3 and longer-term research):

- a tablet with its own internal chip connected to a MANET;
- a tablet tethered to a TP-LINK[3] connected to the MANET;
- a tablet tethered to a TP-LINK connected to the MANET, and connected to the Internet (as a gateway) with its own internal chip;
- a tablet tethered to a TP-LINK connected to the MANET—the TP-LINK device driver and firmware are modified to support cyber operations such as side-channel [8] establishment; and
- a tablet with its own internal chip connected to the MANET, and tethered to a HackRF to perform sensing operations.

These instances represent combinations of the capabilities that we require in TNO tasks and the capabilities that configurations 1 and 2 (above) allow.

Conclusion

We intend to learn more about the hardware architecture options proposed in [7] by further studying the less expensive and more flexible configurations 1 and 2 (above). This will be accomplished through proof-of-concept work establishing an 802.11 MANET test bed with several instances of radio-plus-tablet Android devices (as described in the Discussion section above). This proof-of-concept work, directly influenced by this contract, will help de-risk the TEC3 demonstrator project and provide valuable lessons-learned.

As a final note, the contract highlighted to us that interest in exploiting COTS Android tablets and software-defined radio technologies is not limited to the military: the hacker community is actively exploring methods of modifying tablet devices, programming inexpensive (portable) software-defined radio platforms, and porting known attack techniques to these devices. The Canadian Armed Forces (CAF) needs to be aware of the potential capabilities that these technologies may offer to a less-well-funded but determined adversary.

[3] TP-LINK is a small 802.11 radio device that can be connected via a USB port to a host tablet display device.

Prepared by: Mazda Salmanian, David Brown and Darcy Simmelink, DRDC – Ottawa Research Centre

References

[1] C4ISR & Networks Staff, Mobile apps for improved tactical situational awareness, December 12 2013. http://www.c4isrnet.com/article/M5/20131211/C4ISRNET04/312110021/

[2] Gillen, M., Loyall, J., Usbeck, K., Hanlon, K., Scally, A., Sterling, J., Newkirk, R., Kohler, R., Beyond Line-of-Sight Information Dissemination for Force Protection, MILCOM 2012.

[3] Ter Louw, M., Krull, M., Thomas, T., Cathey, R., Frazier, G., Weber, M., Automated Execution Control and Dynamic Behavior Monitoring for Android Applications, MILCOM 2013.

[4] Wood, S., Mathewson, J., Joy, J., Stehr, M.O., Kim, M., Gehani, A., Gerla, M., Sadjadpour, H., Garcia-Luna-Aceves, J.J., ICEMAN: A System for Efficient, Robust and Secure Situational Awareness at the Network Edge, MILCOM 2013.

[5] Strayer, T., Kawadia, V., Caro, A., Nelson, S., Ryder, D., Clark, C., Sadeghi, K., Tedesco, B., DeRosa, O., CASCADE: Content Access System for the Combat-Agile Distributed Environment, MILCOM 2013.

[6] Brown, J.D., Salmanian, M., Simmelink, D., Tang, H., Song, R., TEC3 CONOPS DRAFT, DRDC-RDDC-2014-R-XXX, submitted for publication, February 2014.

[7] Henderson, G., Pace Bill, Emerging Radio and MANET Technology Study: Research Support for a Survey of State-of-the-art Commercial and Military Hardware/Software for Mobile Ad hoc Networks, DRDC Contract Report CR 2014-xxx, Bell Canada, submitted for publication, February 2014.

[8] Salmanian, M. and Li, M., A high throughput covert overlay network within a MANET, IEEE MILCOM 2013, DRDC Ottawa SL 2013-035.

Distribution list

Major Janus Cihlar, Director Land Requirements (C Army DLR),

Major Ryan Grant, ADM(Mat) Director Soldier Systems Program Management (DSSPM),

Major Daniel Kucherhan, Canadian Forces Support Unit (CFSU),

Major John Pavelich, Technical Officer, Chief of Force Development (DG Cyber),

Dr. Julie Lefebvre, Director General Science and Technology Joint Force Development (DGSTJFD).

This Scientific Letter is a publication of Defence Research and Development Canada. The reported results, their interpretation, and any opinions expressed therein, remain those of the authors and do not necessarily represent, or otherwise reflect, any official opinion or position of the Canadian Armed Forces (CAF), Department of National Defence (DND), or the Government of Canada.